



CVE-2016-6484

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-6484
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2018-10-09 20:00:00 UTC
Description	CRLF injection vulnerability in Infoblox Network Automation NetMRI before 7.1.1 allows remote attackers to inject arbitrary I

Risk And Classification

Problem Types: CWE-93

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Infoblox	Netmri	All	All	All	All

References

Reference

- Infoblox Network Automation CVE-2016-6484 HTTP Response Splitting Vulnerability
- SecurityFocus
- Infoblox 7.0.1 CRLF Injection / HTTP Response Splitting ≈ Packet Storm
- NetMRI Input Validation Flaws Let Remote Users Conduct Cross-Site Request Forgery, HTTP Response Splitting, and Cross-Site Scripting At
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)